



**DEPARTMENT OF THE ARMY**  
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX  
75 6TH AVENUE  
FORT KNOX, KENTUCKY 40121-5717

REPLY TO  
ATTENTION OF:

Expires 17 October 2008

IMSE-KNX-IMA (25)

17 October 2006

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters  
Commanders, Fort Knox Partners In Excellence  
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy No. 49-06 – Information Assurance (IA) Event Handling and Response

1. References.

- a. AR 380-53, Information Systems Security Monitoring, 29 Apr 98.
- b. AR 25-2, Information Assurance, 14 Nov 03.
- c. AR 25-1, Army Knowledge Management and Information Technology, 15 Jul 05.
- d. AR 190-40, Serious Incident Report, 9 Feb 06.
- e. RCERT-CONUS [http://www.rcert-c.army.mil/report\\_incidents\\_index.html](http://www.rcert-c.army.mil/report_incidents_index.html).

2. Purpose. Potential threats to the Fort Knox Campus Area Network (FKCAN) infrastructure have increased with emerging viruses, hacking attacks, and other threats that adversely affect networks. With expansion of interconnectivity in government systems and global information infrastructures, the need for incident prevention and quick responses to threats and intrusions are crucial. An IA event is an assessed event of attempted entry, unauthorized entry, and/or an attack on information systems, to include unauthorized probing, browsing, disruption, or denial of service. It also includes altered or destroyed input; processing; storage; output information; or changes to hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent (e.g., malicious logic). This Incident Response Plan (IRP) is the formal directive on how to respond to an IA event affecting the FKCAN infrastructure when it is discovered and the timely action taken for reducing impact to the FKCAN infrastructure. This enables continued functioning of the infrastructure and prevents recurrences.

3. Scope. Each unit is responsible, through the chain of command, for IA event handling and response procedures by complying with IA responsibilities outlined in ARs 25-1, 25-2, and 380-53; published Best Business Practices; CIO/G-6 guidance; applicable Fort Knox and local organization policies; and as specifically noted below:

IMSE-KNX-IMA

SUBJECT: Fort Knox Policy No. 49-06 – Information Assurance (IA) Event Handling and Response

a. Installation Information Assurance Manager (IAM).

- (1) Establishes an installation IA event reporting system,
- (2) Monitors and performs security auditing on the FKCAN infrastructure devices,
- (3) Logs, investigates, and reviews reported FKCAN infrastructure IA events (central point of contact for IA events and reporting), and
- (4) Works with Regional Computer Response Team (RCERT)/Army Computer Emergency Response Team (ACERT) until the IA event is resolved.

b. Information Assurance Security Officer (IASO), Information Management Officer, system administrator, and Network Manager.

- (1) Installs and maintains security control mechanisms, account management, and auditing capabilities,
- (2) Ensures auditing tools are in place and configured properly in accordance with a coherent auditing strategy and that audit data is reviewed daily,
- (3) Notifies their chain of command and the installation IAM of any IA event per AR 25-2 and this IRP,
- (4) Works with the installation IAM to resolve any security issues pertaining to the network,
- (5) Monitors all systems within their responsibility to ensure that all applicable patches (IA vulnerability assessment, vendor, and those publicly announced) are from reputable/trusted sources,
- (6) Maintains responsibility for the proper security configuration and operation of any device they connect to the FKCAN.

c. Managers and Supervisors.

- (1) Implements requirements for IA event reporting within their assigned area of management control.
- (2) Ensures security violations and incidents within their assigned area of management control are reported to the installation IAM.

IMSE-KNX-IMA

SUBJECT: Fort Knox Policy No. 49-06 – Information Assurance (IA) Event Handling and Response

d. All Authorized Users.

(1) Terminates any session in which a security anomaly is noted or suspected.

(2) Reports actual or suspected security violations or incidents to their supervisor and IASO.


4. Policy.

a. The ACERT, RCERT for the continental United States (RCERT-CONUS), and Fort Knox DOIM monitors the FKCAN for intrusions, suspicious or unauthorized activity, and policy violations. Paragraph 5-7 of AR 25-1 and Section VIII of AR 25-2 provides reporting procedures and responsibilities for all organizations and individuals utilizing devices connected to the CAN. Each party must perform his/her function per these guidelines in order to minimize potential for damage to the network.

b. There are eight categories of IA events. Each is identified with specific descriptions, responses, and recovery. Enclosure 1 lists the types of incidents and the appropriate response to take.

FOR THE COMMANDER:

Encl

  
MARK D. NEEDHAM  
COL, AR  
Garrison Commander

DISTRIBUTION:

A

# INFORMATION ASSURANCE CATEGORY/DESCRIPTION/RESPONSE/RECOVERY

Cat	Response Time	Notification Sender			Description	Severity	Response	Recovery
		1st	2nd	3rd				
1	2 hours	DOIM IA office	DOIM	Garrison CDR	Successful host compromise (unauthorized privileged access). This is a root or administrator level compromise of host. A successful event of this nature means the intruder has total control of the host and access to any and all data stored on it or on systems that trust this host to connect	Serious	The system must be disconnected from the network. It should NOT be turned off. No action should be taken to investigate this incident or change anything on the system unless directed to do so by the DOIM IAM, DOIM IA office, RCERT-CONUS, ACERT, or CCIU. An IP block of the compromised system may be implemented by RCERT CONUS or the DOIM IA office. DOIM completes and submits RCERT Incident Reports and damage assessment checklist (FK Form 5074-E) for all Categories 1 and 2 IA Events. The DOIM forwards report to the Garrison Commander.	Do not start recovery procedures until directed to do so by RCERT-CONUS or ACERT. Normal recovery procedures from an event of the category is to rebuild the system from known good sources, install all required patches, and ensure it is IAVA compliant before reattaching to the network. Notify the DOIM IA office to arrange for a verification scan to be conducted by them and/or RCERT-CONUS.
2	2 hours	DOIM IA office	DOIM	Garrison CDR	Successful unauthorized user compromise (unauthorized limited (user) access). This is a user level compromise. A successful event of this nature means the intruder has access to data, applications, and systems to which the user is allowed access.	Significant	Disconnect the system from the network. It should NOT be turned off. No action should be taken to investigate this incident or change anything on the system unless directed to do so by the DOIM IAM, DOIM IA Office, RCERT-CONUS, ACERT, or CCIU. An IP block of the compromised system may be implemented by RCERT-CONUS or the DOIM IA office. Complete and submit assessment checklist to the DOIM IAM.	Do not start recovery procedures until directed to do so by RCERT-CONUS or ACERT. Normal recovery procedures from an event of the category is to rebuild the system from known good sources, install all required patches, and ensure it is IAVA compliant before reattaching to the network. Notify the DOIM IA office to arrange for a verification scan to be conducted by them and/or RCERT-CONUS.

# INFORMATION ASSURANCE CATEGORY/DESCRIPTION/RESPONSE/RECOVERY

Cat	Response Time	Notification Sender			Description	Severity	Response	Recovery
		1st	2nd	3rd				
3	NA	DOIM IA office	NA	NA	Attempted unauthorized access (unauthorized unsuccessful attempted access). An unsuccessful attempt to access or compromise an information system. An event of this nature means the intruder attempted a known exploit or attempted to log in to an information system but was not successful in compromising it or in logging in.	Simple	No response is necessary. Report the event and include as much data as possible about the intruder and the attempted compromise or intrusion. Complete and submit assessment checklist to installation IAM. Take no further actions unless directed to do so by the DOIM IA office, RCERT-CONUS, ACERT, or CCIU.	There are no recovery procedures required for this event.
4	NA	DOIM IA office	DOIM	NA	Denial of Service (DoS information attack). Isolation of the installation or a portion of the Fort Knox CAN or the denial of the availability of a system or data. A successful event of this nature means the intruder has successfully denied access to either the entire network or a portion of the network or denied access to critical command and control systems or data.	Serious	Determine the cause if at all possible. Contact the DOIM IA office and Networking Branch of DOIM Operations Division for assistance in determining the source of the attack and removing the threat. Take no further actions unless directed to do so by the DOIM IA office, RCERT-CONUS, ACERT, or CCIU. An IP block of the system or systems causing the DoS may be implemented by RCERT-CONUS or the DOIM.	Review logs and configurations to determine if there is anything that can be done to prevent further occurrences of this type of event and/or the cause of the current event.

# INFORMATION ASSURANCE CATEGORY/DESCRIPTION/RESPONSE/RECOVERY

Cat	Response Time	Notification Sender			Description	Severity	Response	Recovery
		1st	2nd	3rd				
5	4 hours	DOIM IA office	NA	NA	Poor security practice. Examples of poor security practices are: root login using telnet, ftp or http; bad passwords; not using secure protocols to transfer sensitive data; downloading programs and patches from foreign repositories and not directly from the vendor; original source or a CONUS repository; Peer-to-Peer (P2P); and Chat (IRC, Instant Messaging, third party chat software, or web based).	Significant	The response depends on the event. The response ranges from disconnection from the network and system rebuild to no action required. Certain circumstances (P2P software in use or non-IAVA compliance for example) may require an IP address block be implemented against the affected system or systems. An IA Event notification is sent to the organization information assurance security officer for the organization to follow appropriate actions (verbal counseling, counseling statement, etc.,).	Follow the instructions or recommendations included with the IA event notification.
6	NA	DOIM IA office	NA	NA	Unauthorized probe or scan. Any automated probe attacks, i.e., SATAN, ISS, etc.,	Simple	Review system event logs and/or network logs to determine if any systems responded to the probe or scan. Contact the DOIM IA office or DOIM Networking Branch for assistance in determining if the scan is unauthorized. An IP block of the address or addresses conducting the scans may be implemented by RCERT-CONUS or the DOIM	Review logs and configurations to determine if any reconnaissance data may have been obtained by the unauthorized scanner

# INFORMATION ASSURANCE CATEGORY/DESCRIPTION/RESPONSE/RECOVERY

Cat	Response Time	Notification Sender			Description	Severity	Response	Recovery
		1st	2nd	3rd				
7	2 Hours	DOIM IA office	DOIM	Garrison CDR	Malicious logic. Any software code intentionally created or introduced into a computer system (that cannot be contained) for the distinct purpose of causing harm or loss to the computer system, its data, or other resources. Examples are adware/spyware, virus, Trojan, worm, etc.,	Serious	Disconnect the system from the network. Do NOT shut the system off. An IP block of the infected system may be implemented by RCERT-CONUS or the DOIM IA office until the system has been found, disconnected from the network, and rebuilt per AR 25-2. Download, complete, and submit the ACERT antivirus report form. A copy of the form and submission instructions can be downloaded from <a href="https://knoxdoim815/portal/imo/antivirus/">https://knoxdoim815/portal/imo/antivirus/</a> . An IA event notification is sent to the organization information assurance security officer for the organization to follow appropriate actions. Most Category 7 reports are not forwarded to the Garrison Commander. Exceptions are Category 7 incidents having high visibility with the Army CIO/G6 or those that have to be reported via SIPRNET.	AR 25-2 states that any system compromised through malicious logic will be rebuilt from original media, patched, and scanned before reintroduction to the network.
8	4 hours	DOIM IA office	NA	NA	Unknown/Under investigation. Use this category until the threat or situation is investigated and a final determination has been made.	Significant	Reassign to the proper category when a final determination is made. An IP address block may be implemented by RCERT-CONUS or the DOIM IA office if the situation warrants. Every attempt will be made to coordinate this with the affected organization, unless a pre-existing agreement to allow blocks of this nature exists.	Recovery is determined after the final determination and IA event category is determined